

REMARKS

Claims 37 through 39 are added. Thus, by this Amendment, Claims 1 through 39 are presented for examination.

The Examiner has rejected all of previously pending Claims 1 through 36 as rendered obvious by the International patent publication of Shultz et al. in view of the United States patent of Carter. In making such rejections he has restated the objections of a prior examiner in which various features taught by the cited prior art references have been selectively combined to argue against the patentability of the claimed invention on a limitation-by-limitation basis.

Applicant's attorney references the telephone interview kindly granted by Examiner Zand on Friday, January 6, 2006. It was Applicant's wish that such interview might lead to a resolution of the issues in the pending application. Applicant's attorney even provided Examiner Zand with proposed claims for discussion (new Claims 37 through 39). The interview was unavailing with the Examiner citing no art but rather asserting that there existed a large amount of prior art that would show the claims presented to be unpatentable. Applicant's attorney advised the Examiner during the interview that he did not

consider the pending rejection of dependent system Claims 26 through 36 to be in compliance with the specificity required of a rejection by Section 706.02(j) of the Manual of Patent Examining Procedures. The Examiner accordingly agreed to issue a proper non-final rejection of all pending claims, citing prior art with the required specificity against the language of each pending claim. Applicant reserves the right to file an appeal covering each and any twice-rejected claim subsequent to receipt of the agreed-upon non-final office action.

The method and system of the claimed invention differ in terms of essential structure from the primary reference upon which the Examiner relies, Schultz et al. This should not be surprising as this reference was brought to the attention of the U.S.P.T.O. upon the filing of the present application which constitutes the United States national phase of International application PCT/EP 99/03839. Schultz was considered during International Preliminary Examination of PCT/EP 99/03839. The International Preliminary Examination Report on August 30, 2000 that resulted which was positive with regard to novelty, inventive step and industrial applicability. A copy of the Report was filed with the U.S.P.T.O. upon entry into the U.S. national phase and is available for the Examiner's review.

Schultz et al. discloses a system (Global Electronic Medical Record "GMR") in which a single level of authorization is required to obtain both data entry into and access to (by provision of the subscriber's network address (= authorization) and password(s)) a subscriber's (i.e. patient/ owner) medical and personal data. (See, for example Figure 4, the final paragraph of claim 1, page 50, lines 27 through 30 and page 52, lines 2 through 7.) The GEMR is organized and arranged for accessing over an electronic network to aid travelers who may be struck by a serious illness while away from home and may have even lost consciousness. At page 4, lines 8-11 Schultz et al. proposes that the system offer access by means of wrist emblem, a neck emblem or a card providing a subscriber's authorization information, including password, to allow a physician to quickly and easily gain access to the afflicted person's medical records without the patient's or other authorized consent.

Unlike Schultz et al., the claimed invention provides both a method and a system that with inherent close control of data. In Schultz et al., the subscriber (patient), has control of all passwords required to access any portion of his GEMR. As such, he may choose to access all of the same medical information that he might otherwise make accessible to a physician. This

cannot occur in a method or system in accordance with the claimed invention. Referring specifically to independent method Claim 1, such claim defines a method for secured access to data in a network including an information center and a plurality of data area access systems in which permission to store said data and to define, at the information center, access rights of third parties to said is limited to the owner of the rights to said data. Such method includes, among other limitations, "in each case storing the data only once in one of said data area access systems not accessible to the owner of the rights". In the claimed invention an "owner of data" corresponds to a patient while the "third parties" may be thought of as physicians, physicians' offices, insurance companies or others having a potential need for access to the owner's medical information. Such a limitation strictly distinguishes the method claims of the pending application from Schultz et al. in which the subscriber has access to all passwords for accessing his GEMR. Schultz et al. may not be combined with another reference to incorporate the prohibition of access to the owner of data as it "teaches away" from any such limitation.

Similar distinguishing limitations are found in the system claims. Independent Claim 25 is directed to a system that

includes, among other limitations, "said system is configured and adapted such that access to any piece of data entered into the system is restricted to those authorized users of the system having appropriate access rights as defined by said information for the piece of data to be accessed." In the system of the claimed invention, only a patient or owner of data ("authorized user of said information center") may define a physician, physician's office, insurance company or other entity with potential interest in access to his data ("authorized user of data area access system") as eligible to receive data from another data area access system. As the above language of independent system Claim 25 makes clear, while the authorized user of the information center (corresponds to the "subscriber" of Schultz et al.) can control the sharing of his medical records, he is prohibited access to his records within the context of the claimed system. Again, this is entirely contrary to Schultz et al.

Dependent system Claim 28 further explicitly limits the data area access systems to operation in a mode "in which an authorized user of said information center who is not an authorized user of the respective data area access system...cannot access any pieces of data entered into the

system". New dependent Claim 39 likewise includes, among other limitations, "said system is configured and adapted such that access to any piece of data entered into the system is restricted to those authorized users of the data area access systems having appropriate access rights ad defined by said information for the piece of data to be accessed.

The limitation of the method and system of the invention, in contrast to Schultz et al., to prevent the data owner's access to medical or other records stored within the various data area access systems permits greater candor on the part of the physician as notations of matters such as personal observations of psychological influences on the patient's health cannot be accessed by the owner of the data/authorized user of the information center via the system and method of the invention. This is entirely and conceptually unlike Schultz et al. in which the subscriber may make a complete inspection of all data pertaining to himself that is accessible to physicians through his GEMR.

Another significant distinction between the claimed invention and Schultz et al. is made explicit in independent system Claims 25 and 37. Each includes, among other limitations,

"said system is configured and adapted such that entry of a piece of data into said system comprises a writing of said piece of data to a respective one of said secure data memories that can only be effected by an authorized user of the data area access system associated with the respective secure data memory and in conjunction with the authorization of an authorized user of said information center". As discussed above, an authorized user of a data area access system will generally be a medical care provider, his office or an insurance company, each with an interest and need for access to certain records stored at one or more of the data area access systems of the system of the invention which the authorized user of the information center is the patient-data owner (corresponding to the subscriber of Schultz et al.) The feature defined by this limitation permits the patient (authorized use of information center) to participate in the entry of portions of his medical records in consultation with the medical care provider (authorized user of data area access system). This is unlike and contrary to Schultz et al. in which no such provision is made for the patient to, in effect, "edit" the extent of his medical data that may be made available to other physicians (authorized users of data area access systems) within the system. This is entirely within the concept of the present invention as only the patient himself can

authorize the information center to permit the access of other data area access systems to particular sources of his information. When granting such access rights, the patient may take into account the content of records stored at a particular data area access system. For example, the data owner might not want an insurance company or a relative-physician to be aware of psychological matters discussed with a data area access system where he was treated for unrelated medical issues. As the invention bars data access without the patient's explicit consent, it permits ready tracing of those attempting to gain unauthorized access to data entered into the system for reprimand or exclusion from the system.

Schultz et al. fails to teach or suggest the claimed features of independent Claims 1, 25 and 37, to wit, "access rights of third parties to said data is limited to the owner of rights to said data" and "said information center is configured and adapted such that display and modification of the information defining the access rights to said entered piece of data is restricted to said authorized user of said information center". Such structure and operation are clearly contrary to Schultz et al. See, for example, at page 36, lines 28 through 30, where

Schultz et al. states "the security passport may be changed by the subscriber or an authorized technician".

In addition to the points of clear distinction between the invention as claimed and the primary reference, comment is directed to the pending rejections insofar as dismissal, as a mere design choice, of the claim limitation that includes "storing the data only once". Such a limitation reflects numerous unforeseen advantages over the prior art as it characterizes a system that does not include replicated data. This gives the data the quality of "inherent uniqueness" from which numerous significant advantages follow. The system and the method of the invention each benefit from the reliable authenticity and non-repudiability of all of the data stored within the system. Confusion cannot arise with regard to whether two sets of complex data are identical or indeed indicative of separate results. A doctor reviewing a patient's file is thereby assured in the invention (and contrary to the teachings of the cited references) that data is of unambiguous significance and not subject to doubt. He knows, for example, that seemingly identical lab results needn't be doubted as possibly resulting from error as, in the claimed system, they cannot be mere replicas of one another that arrived from different areas of the


system. Rather, he can confidently proceed without doubt as to the significance of each set of data. This obviates any need to undertake costly reviews of data for certainty of interpretation.

The elimination of any possibility of duplicate data within the system of the invention permits "watermarking" (see page 17, second paragraph and dependent method Claim 24) so that data transmissions within the system are traceable on the basis of the data itself. This feature is advantageous in uncovering and prosecuting authorized users of the system who exploit access rights in an unauthorized manner.

Storage of data only once also reduces vulnerability of to cyberattacks and other unauthorized access. Violation of one data area access system cannot compromise the security of data stored at other locations in a system in accordance with the claimed invention. As may thus be seen, the absence of replicas within the system of the invention greatly simplifies the control over data access. Accordingly, the Examiner's dismissal of this important limitation as a matter of mere design choice is entirely unsupportable demonstrates a failure to appreciate the significance of this limitation that distinguishes Applicant's claimed invention from the prior art.

For the foregoing reasons, all presently-pending claims define patentable subject matter. Prompt allowance and issuance of such claims are therefore earnestly solicited.

Respectfully submitted,


Elliott N. Kramsky
Registration No. 27,812
Attorney for Applicant

5850 Canoga Avenue, Suite 400
Woodland Hills, CA 91367
Ph: (818) 992-5221
Fx: (818) 710-2751